CIO/NII
Enabling Net-Centric Operations

Mission: Possible
Securely Connecting People With Information

Mr. Robert Lentz

Office of the Assistant Secretary of Defense

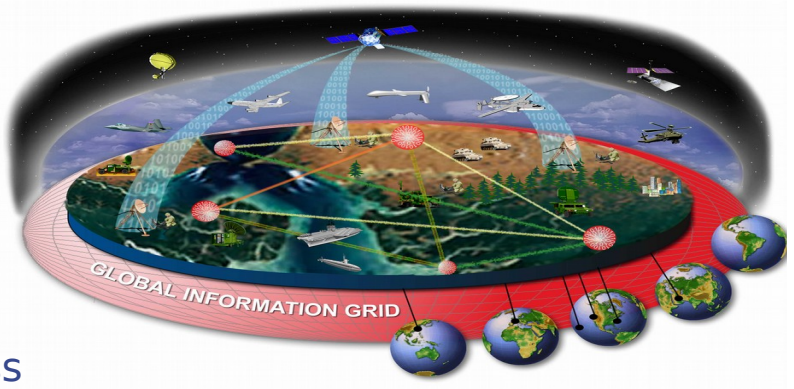
NII / DoD CIO

Director, Information Assurance Policy

DoD CIO's strategic direction for creating a secure Net-Centric environment

CIO/NII Enabling Net-Centric Operations

Mission: **Enable Net-Centric Operations** – Lead the Information Age transformation that enhances DoD's efficiency and effectiveness.



Vision: **Deliver the Power of Information** – An agile enterprise empowered by access to and sharing of timely and trusted information.

Goals:

1. **Build** – Make information available through a network that users know they can trust
2. **Populate** – Add new dynamic sources of information to use in defeating adversaries
3. **Operate** – Maintain systems and keep the networks fully functional at all times
4. **Protect** – Implement new and better ways to eliminate weaknesses

The secured GIG holds the future of warfighting – Net-Centricity will be achieved through the GIG.

CIO/NII
Enabling Net-Centric Operations

A Comprehensive Plan for Securing the GIG

- **Securing the GiG involves four major components:**
  - **DoD's IA Strategic Plan**
  - **Full spectrum GIG operations**
  - **IA component of the GIG Integrated Architecture**
  - **Implementation guidance**
- **The IA Strategic Plan lays the foundation for Securing the GIG:**
  - **The Vision and Goals in the Plan are enduring and serve to define a consistent strategic direction to assuring our information**
  - **We are updating the objectives in the IA Strategic Plan to ensure they are:**
    - Consistent with how the Department's IA program has evolved over the past two years and addressing the QDR imperatives of shoring up today's defenses and focusing on the future
    - Outcome-oriented – reflecting what outcomes we want to achieve
    - Quantifiable and measurable – enabling us to measure our progress and addressing the DEPSECDEF's emphasis on measuring performance
    - Focused on current and relevant strategic issues – enabling us to communicate a compelling story

These actions will secure the GIG and instill user confidence in the information that moves

IA Strategic Plan Framework

VISION
Dynamic Information Assurance
for the Global Information Grid (GIG)

GOALS and OBJECTIVES

QDR Imperative I

Shore Up Today's Defenses!

QDR Imperative II

Focus on the Future!

Goal #1: Protect Information – Safeguarding data as it is being created, used, modified, stored, moved, and destroyed whether at the client, within the enclave, at the enclave boundary, or within the computing environment, to ensure that all information's level of trust corresponds with mission needs.

Goal #2: Defend Systems & Networks – Recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies to ensure that no access is uncontrolled and all systems and networks are capable of self-defense.

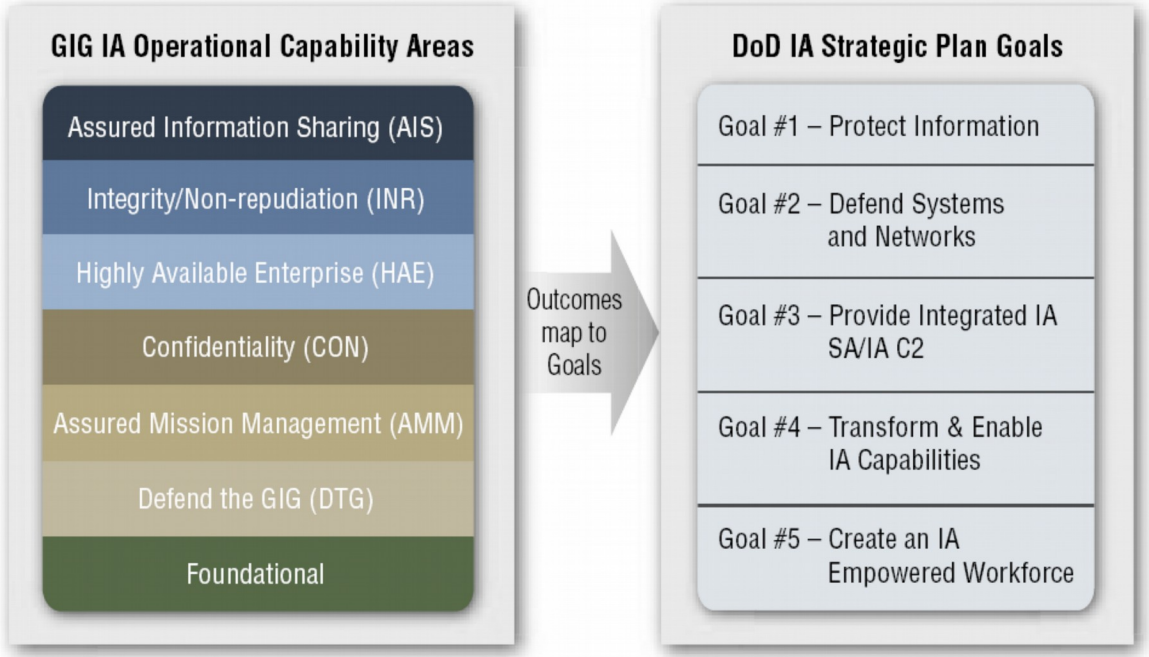
Goal #3: Provide Integrated Situational Awareness/IA Command and Control (C2) – Integrating an IA posture into an operational picture synchronized with NetOps and emerging Joint C2 Common Operating Picture (COP) programs to provide decision-makers and network operators at all command levels with the tools to conduct IA/CND operations and Net-Centric Warfare.

Goal #4: Transform and Enable IA Capabilities – Discovering emerging technologies, experimenting, and refining development, delivery, and deployment processes to improve life cycle time, reduce risk exposure, and increase return on investments.

Goal #5: Create and IA Empowered Workforce – Establish an IA professional workforce with the knowledge, skills, and abilities to effectively prevent, deter, and respond to threats against DoD information, information systems, and information infrastructures and create the capability to place people with the right skills, in the right place, at the right time.

Operationalizing the Plan

- **We are developing an Integrated IA Performance Management Plan to measure how well we are managing the programs and initiatives in the IA Capability Portfolio and our progress against our Strategic Plan**
- **The Integrated IA Performance Management Plan will allow us to link portfolio investments to outcomes – enabling us to demonstrate the value of IA and provide senior leaders the information required to make decisions and effectively manage the IA Portfolio**


GIG IA Operational Capability Areas
Assured Information Sharing (AIS)
Integrity/Non-repudiation (INR)
Highly Available Enterprise (HAE)
Confidentiality (CON)
Assured Mission Management (AMM)
Defend the GIG (DTG)
Foundational
Outcomes map to Goals
DoD IA Strategic Plan Goals
Goal #1 – Protect Information
Goal #2 – Defend Systems and Networks
Goal #3 – Provide Integrated IA SA/IA C2
Goal #4 – Transform & Enable IA Capabilities
Goal #5 – Create an IA Empowered Workforce

CIO/NII Enabling Net-Centric Operations

CIO/NII
Enabling Net-Centric Operations

Mission: POSSIBLE

- **The GIG is the future of secured information for our Armed Services**
- **When fully deployed and mature, it will serve as the Net-Centric source of trusted on-demand data and intelligence required by our Joint, Allied, and Coalition Forces to achieve full-spectrum dominance**
- **A strong and deliberate IA strategy, governance, and implementation plan that includes personal vigilance on the part of us all is needed to secure the GIG and ensure that sensitive information is both trusted and secure**
- **A secured GIG can only be achieved with the dedication and commitment of everyone**
- **To be effective, Commanders must establish the climate, commit resources, organize and train personnel, and accept responsibility for protecting the GIG**

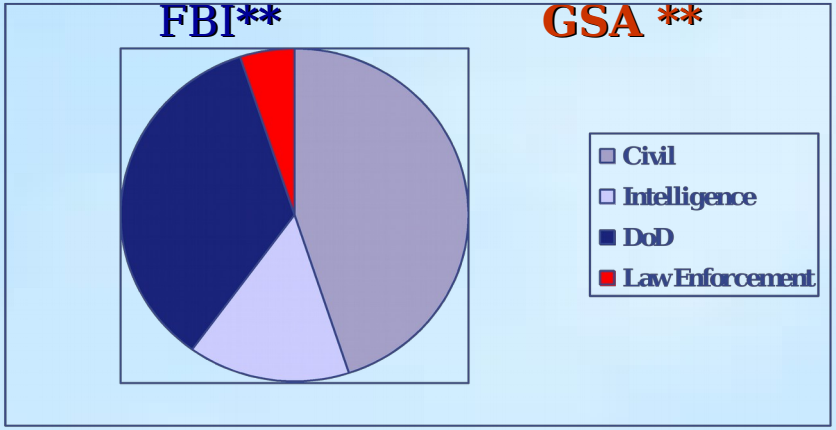
Committee on National Security Systems

GSA Jul06

MEMBERSHIP

- **CHAIR: John Grimes, Chair, ASD (NII)/DOD CIO**

State		Defense	Treasury**	JCS
Attorney General**	Army	Commerce	Navy	
Transportation**	Air Force		Energy**	
Marines				
OMB	NSA	NSC	DNI	
DIA	FBI**	GSA **	DHS	
CIA				



- **CNSS Observers**

DISA	FCC	NGA	NASA	NRO
NIST**	NARA	ISOO	NRC	

**Some functions transferred to DHS

MILESTONES IN OUR HISTORY

- **PRESIDENTIAL DIRECTIVE, OCTOBER 1952**
  - **- COMSEC: a national responsibility**
  - **-SECDEF = Executive Agent**
- **NSDD 145, SEPTEMBER 1984**
  - **- Computer security: a national responsibility**
  - **- Telecommunications and AIS security become DoD responsibility**
  - **- DIRNSA = National Manager**
- **P.L. 100-235, COMPUTER SECURITY ACT, JANUARY 1988**
  - **- Government-wide computer security: national priority**
  - **- NIST = most unclassified; NSA = other + technical advice**
  - **- NIST: develop standards and guidelines with NSA's assistance**
- **NSD-42, July 1990**
  - **-Complied with P.L. 100-235**
- **-E.O. 13231, October 2001**
  - **-CNSS is Standing Committee under the President's Critical Infrastructure Protection Board**
- **-E.O. 13286, March 2003**
  - **-Retain CNSS as established by and consistent with NSD-42**

NSD-42 Authorizes the CNSS to Secure National Security Systems by:

- Providing a forum for discussion and development of National Security Policy
- Assessing the health of National Security Systems
- Approving the release of INFOSEC products and information to foreign governments
- Partnering with other security fora (NSTAC and CIO Council, etc)

Accomplishments

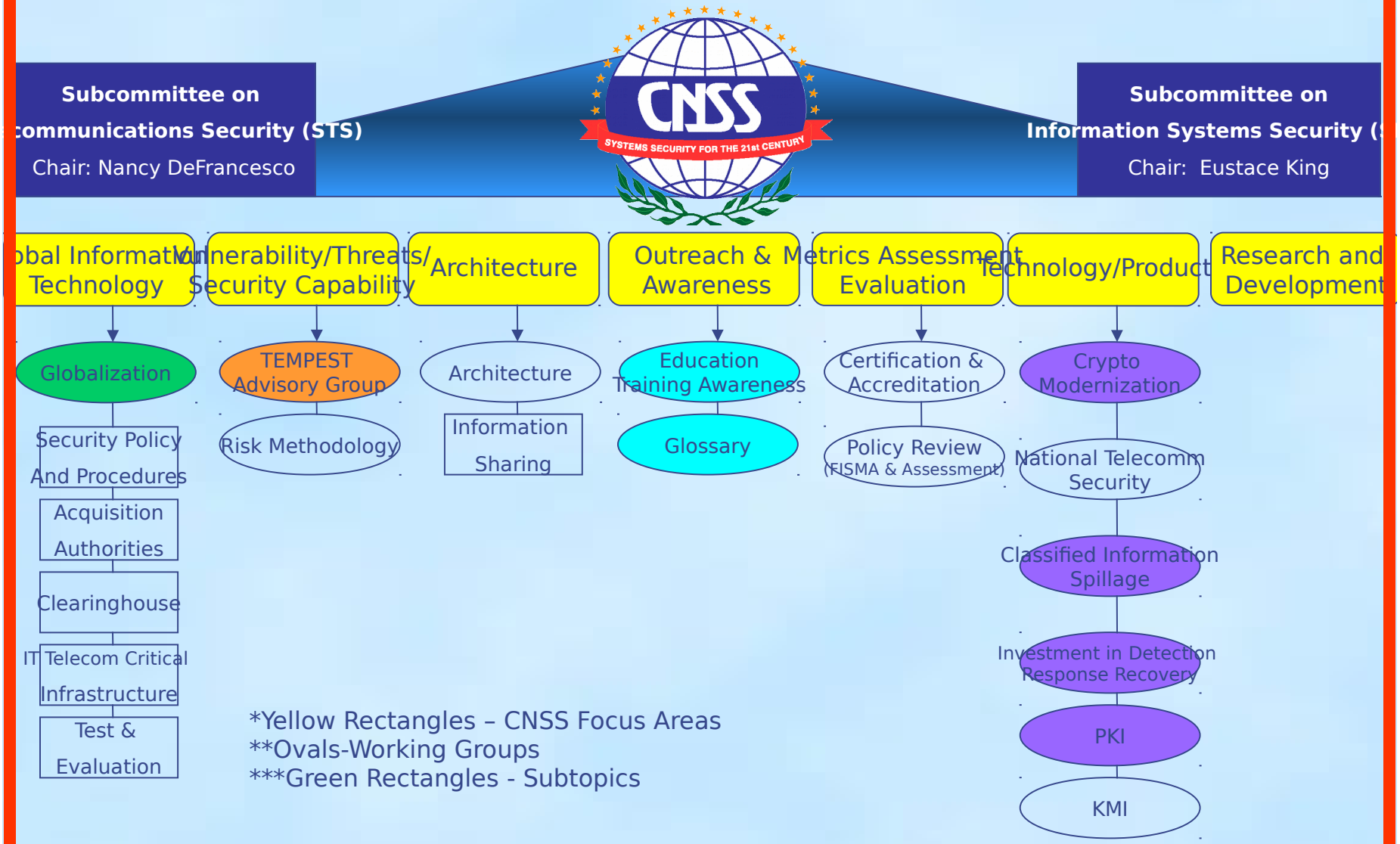
- Recent Issuances
  - Wireless Capabilities Policy
  - Classified Information Spillage Policy
  - Education, Training, and Awareness Directive
  - National IA Glossary
  - Assessment of IA National Security Systems

- In Development
  - Architecture Policy
  - Globalization IT Report
  - Investment in Detection, Response & Recovery Policy Draft

2006 NATIONAL SECURITY SYSTEMS (NSS) ASSESSMENT RECOMMENDATIONS

- **Develop Cyber National Intelligence Estimate**
- **Review policy structure to protect NSS Information**
- **Develop strategy for foreign acquisition of U.S. IT producers and service providers**
- **Invest in developing security tools**
- **Develop more robust Certification and Accreditation (C&A) process**
- **Create patch management system**
- **Invest resources to replace aging cryptographic equipment (CIOs)**
- **Develop career paths for graduates of Centers of**

CNSS Focus Areas and Organization



*Yellow Rectangles – CNSS Focus Areas
**Ovals-Working Groups
***Green Rectangles - Subtopics

EXECUTIVE SECRETARY

Sharon Shoemaker, Acting

Phone: (410) 854-6906

CNSS Secretariat Manager

Elaine Gist

Phone: (410) 854-6805

Fax: 410-854-6814

Secure fax: (410) 854-6805

cnss@radium.ncsc.mil

CNSS Home Page

http://www.cnss.gov

CIO/NII
Enabling Net-Centric Operations

Mission: Possible
Securely Connecting People With Information

Mr. Robert Lentz

Office of the Assistant Secretary of Defense

NII / DoD CIO

Director, Information Assurance Policy

CIO/NII
Enabling Net-Centric Operations

Back-up Slides

CIO/NII
Enabling Net-Centric Operations

Goal #1: Protect Information

Goal #1: Protect Information – Safeguarding data as it is being created, used, modified, stored, moved, and destroyed whether at the client, within the enclave, at the enclave boundary, or within the computing environment, to ensure that all information's level of trust corresponds with mission needs.

Objectives

- Assure information sharing and collaboration within DoD and with other Agencies, allies, coalitions, and partners
- Render data unusable/unreadable when accessed by other than trusted parties whether it is in transit or at rest
- Improve mission management security, balancing the implementation of features within a given processing environment to meet the security and mission needs
- Protect and assure the availability of information in austere environments

Key Programs & Initiatives

- IA Component of GIG Architecture
- Cryptographic Modernization
- Metadata Standards
- IPv6
- IA Component Management
- HAIPE IS
- NCES
- GIG-BE
- TSAT
- WIN-T
- AEHF
- Cross Domain Solutions
- Data at Rest
- KMI / EKMS
- Identify Management
- PKI / PKE / CAC
- Biometrics

Key Accomplishments

- Launched the Cryptographic Modernization Program
- Implemented DoD PKI to provide higher trust in identities and improve protection of sensitive data
- Established DoD/IC Unified Cross Domain Management Office (CDMO)
- Issued the IA Component of the GIG Integrated Architecture Version 1.1, providing a GIG IA vision aligned to the GIG IA Initial Capabilities Document

Goal #2: Defend Systems & Networks

Goal #2: Defend Systems & Networks – Recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies to ensure that no access is uncontrolled and all systems and networks are capable of self-defense.

Objectives

- Protect GIG systems and information from cyber-attack
- Detect cyber-attacks and misuse
- Protect GIG systems and information from cyber-attack
- Detect cyber-attacks and misuse
- Provide continued access to and use of mission critical, high priority services while under a cyber-attack
- Restore and react to degraded services (in priority order) after a cyber attack has been contained

Key Programs & Initiatives

- ESG Architecture
- CND Component of GIG IA Architecture
- DoDI 8552 – Mobile Code
- DoDD 8551 – Ports & Protocols
- DoD IA & CND Steering Group Initiatives
- 8530.1 & .2 Update
- CND Service Provider C&A Program
- CND Assessment
- DMZ Implementation
- CND Program Plan
- IAVM Implementation (SCCVI, SCRI, SDEP)
- SIPRNet Protection HBSS
- ESG – Tier 3 SIM
- Wireless Network Defense
- CND RA Tools for Attribution & Traceback
- Insider Threat Mitigation

Key Accomplishments

- Established a DoD CND Enterprise Solutions Steering Group to acquire, field, and sustain enterprise CND tools
- Implemented automated, enterprise-wide vulnerability management capability to perform automated cyber vulnerability scanning and automated patching

CIO/NII Enabling Net-Centric Operations

Goal #3: Provide Integrated SA / IA C2

Goal #3: Provide integrated situational awareness/IA Command and Control (C2) – Integrating an IA posture into an operational picture synchronized with NetOps and emerging Joint C2 Common Operating Picture (COP) programs to provide decision-makers and network operators at all command levels with the tools to conduct IA/CND operations and Net-Centric Warfare.

Objectives

- Improve IA SA for NETOPS through improved detection and response times
- Synchronize CND with other CNO mission areas
- Assess policy compliance and the IA posture of all DoD Components
- Improve information sharing and security planning across Federal departments, critical infrastructures, international partners, and the private sector
- Standardize, certify, and accredit all CND Service Providers

Key Programs & Initiatives

- AS&W Deployment
- ESG Plan Development
- I&W
- IA User-Defined Operational Picture (UDOP)
- IA/NetOps C2
- CND RA
- International CND Operations
- National Cyber Response Action Improvement

Key Accomplishments

- Created substantial improvements in attack, sensing, and warning capabilities through an enhanced constellation of intrusion and anomaly detection sensors
- Established successful international partnerships increasing critical CND information sharing for enhanced IA/CND programs
- Aligned over 83% of DoD Components to an accredited CND Service Provider

CIO/NII Enabling Net-Centric Operations

CIO/NII
Enabling Net-Centric Operations

Goal #4: Transform & Enable IA Capabilities

Goal #4: Transform and Enable IA Capabilities – Discovering emerging technologies, experimenting, and refining development, delivery, and deployment processes to improve life cycle time, reduce risk exposure, and increase return on investments.

Objectives

- Improve the management and performance of the GIG IA Portfolio
- Improve the management and performance of the IA R&D portfolio
- Improve the processes for development and delivery of IA capabilities
- Improve organizational and operational innovation, responsiveness, and productivity (achieved through knowledge management)
- Mitigate IA risk throughout the lifecycle of all DoD programs
- Mitigate the IA risks brought about by IT

Key Programs & Initiatives

- Net-Ready KPP
- IA Acquisition Process Integration
- IA Assessments
- IA Strategy Development & Process
- Software & Hardware Assurance
- NIAP Re
- IA Policy Framework Management
- IA Performance Metrics
- Commercial Innovation Interface Venture Capital Initiative (DDRE)
- National Disclosure Policy Review
- International IA Strategy
- IA Portal
- eMASS Pilot
- Multi-National Info Sharing
- DITSCAP Update to DIACAP

Key Accomplishments

- Increased Systems Accreditation rate while increasing number of systems reported in IT Registry
- IA is a regular part of major DoD exercises
- Expanded Red and Blue Team evaluation activities across DoD to enhance mission readiness
- Established GIG IA Portfolio
- GIAP) Management Office, to oversee the IA Capability Portfolio and maximize the IA investments enterprise-wide

CIO/NII
Enabling Net-Centric Operations

Goal #5: Create an IA Empowered Workforce

Goal #5: Create and IA Empowered Workforce – Establish an IA professional workforce with the knowledge, skills, and abilities to effectively prevent, deter, and respond to threats against DoD information, information systems, and information infrastructures and create the capability to place people with the right skills, in the right place, at the right time.

Objectives

- Certify all personnel performing IA functions to baseline IA skill standards
- Fill identified IA positions with trained and certified IA personnel
- Enhance knowledge and skills on a continual basis
- Educate personnel on the impact of IA on business operations and mission accomplishment
- Assess operational effectiveness of IA Workforce Improvement Program

Key Programs & Initiatives

- 8570 Implementation
- IA Skills Standards Development (Job Task Analysis- JTA)
- Certification Industry Partnership
- IA Training Products Development
- IA Workforce Outreach Communication Plan
- Personnel Database Upgrades
- Pilot for Tracking Certification Data
- Evaluate S/A Training
- DoD IA Scholarship Program (IASP)
- PME Instruction Update; Reaching Non-IA Leadership

Key Accomplishments

- Established a Department-wide standard for IA workforce management and baseline IA knowledge and skills that all personnel performing IA functions must achieve
- Facilitated development of a system administration network attack simulation trainer
- Trained the majority of DoD personnel in computer security awareness despite larger numbers of Service members deployed to combat theaters
- Expanded the number of universities that are CAEs in IA Education to over 75
- Institutionalized DoD IASP to attract and retain top talent and to target academic research

CIO/NII
Enabling Net-Centric Operations

DoD has realized several significant accomplishments across each of the five goals

- Launched the Cryptographic Modernization Program
- Implemented DoD Public Key Infrastructure (PKI) to provide higher trust in identities and improve protection of sensitive data
- Established a DoD Computer Network Defense (CND) Enterprise Solutions Steering Group to acquire, field, and sustain enterprise CND tools
- Implemented automated, enterprise-wide vulnerability management capability to perform automated cyber vulnerability scanning and automated patching
- Created substantial improvements in attack, sensing, and warning capabilities through an enhanced constellation of intrusion and anomaly detection sensors
- Established successful international partnerships increasing critical CND information sharing for enhanced IA/CND programs
- Established a Department-wide standard for IA workforce management and baseline IA knowledge and skills that all personnel performing IA functions must achieve
- Issued the IA Component of the GIG Integrated Architecture Version 1.1,
- Facilitated development of a system administration network attack simulation trainer
- Established DoD/IC UnifiedCross Domain Management Office (CDMO)
- Increased Systems Accreditation rate while increasing number of systems reported in IT Registry
- Trained the majority of DoD personnel in computer security awareness despite larger numbers of Service members deployed to combat theaters
- Expanded the number of universities that are Centers of Academic Excellence in IA Education to more than 75
- Institutionalized DoD IA Scholarship Program (IASP) to attract and retain top talent and to target academic research to support the mission critical IA/IT needs of the Department
- Expanded Red and Blue Team evaluation activities across DoD to enhance mission readiness■ IA is a regular part of major DoD exercises
- Aligned over 83% of DoD Components to an accredited CND Service Provider
- Established the GIG IA Portfolio (GIAP) Management Offi ce, to oversee the IA